VIRDI 4000 Guía de Usuario

Versión esp-1.00

< Glosario>

- Admin, Administrador
  - Como usuario que puede acceder al modo menú del terminal, puede registrar/modificar/borrar usuarios del terminal y alterar el entorno de funcionamiento modificando los parámetros de configuración.
  - Si no hay un administrador registrado para el terminal, cualquiera puede acceder al menú del dispositivo y cambiar la configuración. Por lo tanto, es recomendable registrar al menos un administrador.
  - Muestre especial cuidado para el registro y la operativa ya que un administrador tiene privilegios para cambiar parámetros importantes del terminal.

- Autentificación 1:1
  - Las huellas dactilares del usuario se comparan con las huellas previamente registradas.
  - Este método se denomina 1 a 1 porque solo la huella dactilar asociada al usuario previamente localizado (por presentar una tarjeta o introducir un ID) se compara con la presentada.

- Autentificación 1:N
  - Este es un método que busca el usuario correspondiente solo con la huella dactilar.
  - Este método se llama autentificación 1 a N debido a que busca una huella dactilar idéntica entre todas las huellas registradas, sin que se introduzca previamente un ID de usuario o se presente previamente una tarjeta.

- I-Captura (Captura inteligente)
  - Refuerza la capacidad de detección de huellas dactilares (huellas residuales dejadas sobre la ventana del sensor debido al sudor o contaminantes del dedo) y ajusta automáticamente la configuración de los sensores para detectar huellas dactilares de buena calidad, independientemente de las condiciones (seco o húmedo).

- Nivel de autentificación
  - Este es el nivel utilizado para la autentificación de la huella dactilar, comprendido entre 1 y 9, que permite comparar la huella registrada previamente con la presentada. La autentificación sólo tiene éxito cuando la similitud entre ambas huellas es superior al nivel de seguridad preseleccionado.

- A mayor nivel de autentificación, mayor será la seguridad. Sin embargo, como requiere un índice de coinciencia relativamente más alto, puede dar lugar a falsos rechazos.
- Nivel 1:1: Nivel de autentificación utilizado para la verificación 1:1.
- Nivel 1:N: Nivel de autentificación utilizado para la verificación 1:N.

● Método de autentificación

- Representa los distintos tipos de autentificación, incluyendo la autentificación FP (huella dactilar), autentificación RF (tarjeta), autentificación por clave o combinación de varios métodos. Por ejemplo: Card o FP: autentificación con tarjeta o huella dactilar. En este ejemplo se podría utilizar una tarjeta en el supuesto caso de que fallara la huella dactilar.

● Teclas de función

- Las teclas [F1], [F2], [F3], [F4] están disponibles. Se usan para una autentificación de forma directa y cada tecla representa un modo de autentificación.

Índice

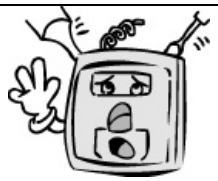
< Glosario> 2
1. Instrucciones previas al primer uso 6
1.1. Precauciones de seguridad 6
1.2. Descripción del terminal 8
1.4. Pantalla 9
1.5. Información de voz durante la autentificación 10
1.6. Sonidos durante la autentificación 10
1.7. Señales LED 10
1.8. Correcto registro de huellas dactilares y métodos de entrada 11
2. Introducción 13
2.1. Características 13
2.2. Configuración 16
2.2.1. Configuración de la red 16
2.2.2. Configuración autónoma 16
2.3. Especificaciones 17
3. Configuración 18
3.1. Comprube el producto antes de configurarlo 18
3.1.1. Menu 18
3.1.2. Cambiar configuración 18
3.1.3. Guardar configuración 19
3.2. Configuración del menú 20
3.3. Usuario 22
3.3.1. Registro de usuario 22
3.3.2. Eliminar usuario 27
3.3.3. Modificar un usuario 27
3.3.4. Registro del administrador 31
3.3.5. Eliminar usuarios 31
3.4. Configuración de la red 32
3.4.1. Número ID del terminal 32
3.4.2. Modos de conexión [NS / SN / NO] 32
3.4.3. Configuración del método de conexión 33
3.4.4. Configuración de la direccion IP 33
3.4.5. Configuración de la mascara de subred 33
3.4.6. Puerta de enlace 34
3.4.7. IP del Servidor 34
3.4.8. Puerto del servidor 34
3.5. Ajustes 36
3.5.1. Application mode settings 36
3.5.2. Ajustes de métodos de autentificación 38
3.5.3. Puerta / Cerradura 41
3.5.4. Volumen 42
3.5.5. Hora actual 43
3.5.6. Otros ajustes 43
3.6. Información del terminal 45
3.7. Funciones ampliadas 46
3.7.1. Ajustes de bloqueo del terminal 46
3.8. Configuración del dispositivo 47

3.8.1. Teclas de función 47
3.8.2. Lector de tarjetas 48
3.8.3. Sensor de huellas dactilares 48
3.8.4. Wiegand output settings 50
3.8.5. Configuración del sistema 51
3.8.6. Inicialización del terminal 52
4. Usos del terminal 53
4.1. Control de acceso 53
4.1.1. Modo de autentificación 53
4.1.2. [1:1] Autentificación con huella dactilar 54
4.1.3. [1:N] Autentificación con huellas dactilares 56
4.1.4. Autentificación con contraseña 57
4.1.5. Autentificación con tarjeta 59
4.1.6. Autentificación de ID de grupo 61
4.1.7. Autentificación de huellas digitales múltiple 62
4.2. Control horario 63
4.2.1. Modo de autentificación 63
4.2.2. Autentificación de huellas dactilares [1:1] 64
4.2.3. Autentificacion de huellas dactilares [1:N] 64
4.2.4. Autentificación con contraseña 64
4.2.5. Autentificación con tarjeta 64
4.2.6. Autentificación de ID de 64
4.2.7. Working mode expansion using multi-key authentication 64

1. Instrucciones previas al primer uso

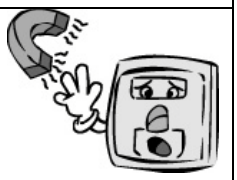
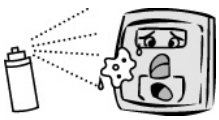
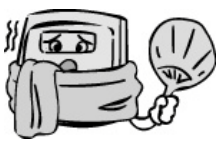
1.1. Precauciones de seguridad

● Advertencias

No manipule la unidad con las manos húmedas y no permita que se vierta ningún líquido dentro. Puede provocar un cortocircuito o daño.		No sitúe una fuente de fuego cerca de la unidad. Puede causar un incendio.	
No desmonte, repare o modifique la unidad. Puede causar un cortocircuito, fuego o daño.		No permita que los niños se acerquen. Puede causar un accidente o daño.	

- Si las instrucciones mostradas no son seguidas, puede causar la muerte o serios daños al usuario.

● Precauciones

Aleje el terminal de una fuente directa de sol. Puede causar mal funcionamiento, deformación o cambio de color de la unidad.		Evite la humedad alta y el polvo. Puede provocar un mal funcionamiento de la unidad.	
Evite utilizar agua, benceno, disolvente o alcohol para limpiar la unidad. Puede provocar un cortocircuito o fuego.		No acerque un imán a la unidad. Puede dañarla o provocar un mal funcionamiento.	
Evite tener el área de captura de huella sucia. Puede provocar una autentificación incorrecta de las huellas dactilares.		Evite utilizar insecticidas o espráis inflamables cerca de la unidad. Se puede deformar o cambiar el color de ésta.	
Evite los golpes y el uso de objetos cortantes en la unidad. Esta puede dañarse o romperse.		No sitúe la unidad en un lugar con cambios bruscos de temperatura. Puede provocar malfuncionamiento de ésta.	

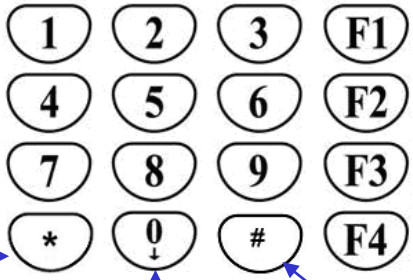
-Si ignora las precauciones arriba referenciadas, puede producirse un

daño o accidente humano.

※Bajo ninguna circunstancia Union Community (Sticard) será responsable de los accidentes o daños provocados por un uso inapropiado del producto. Debe seguir las indicaciones establecidas en esta guía de usuario.

1.2. Descripción del terminal

1.3. Teclado



Entrada

Salida

Fuera

Vuelta

Configuración del menu del terminal (arranca el modo de menú cuando se presiona más de 2 segundos)

Introducir '0' o desplazar el menú LCD hacia abajo

Limpiar un error al introducir los ajustes
Desplazar el menu LCD hacia arriba
Salir del ajuste del menu

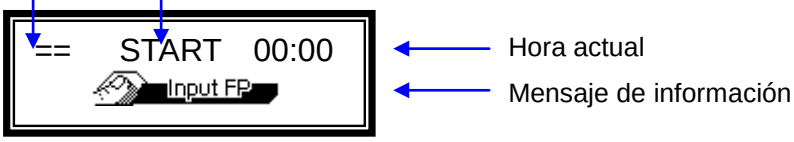
Utilizar después de introducir los ajustes de configuración del terminal.

Utilizar como telefonillo para los visitantes.

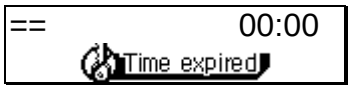
1.4. Pantalla

== Conectado a la red del servidor
→← Desconectado de la red del servidor

Visualizacion de entradas y salidas (F1, F2, F3, F4)



== 00:00 UNION community	- Pantalla de inicio
== 00:00 Input ID	- Entrada ID de un usuario
== 00:00 Input FP	- Entrada huella dactilar
== 00:00 password	- Entrada contraseña
== 00:00 Success	- Autentificación correcta
== 00:00 Matching fail	- Autentificación errónea
== 00:00 No record	- Entrada de ID de un usuario no registrado - El método de conexión es SN y la autentificación 1:N es accesible incluso cuando no hay usuarios permitidos para este tipo de acceso.
== 00:00 Net Error	- Sin respuesta del servidor durante la autentificación. - La red del servidor está desconectada durante el proceso de autentificación.
→← 00:00 Connecting	- Usuario no registrado en el terminal o sin conexión a la red del servidor. Intentando conexión de red.
== 00:00 Place your card	- Entrada de tarjeta

	- Autentificación de usuario registrado fuera del tiempo programado de entrada/ salida.
	- Servidor verificando la autentificación.
	- Terminal bloqueado.
	- Actualizando el terminal. (No se debe apagar el terminal cuando aparece este mensaje)

1.5. Información de voz durante la autentificación

“Por favor, introduzca su huella dactilar”	Coloque su dedo sobre la ventana del escáner de huellas dactilares.
“Está autorizado”	Autentificación correcta
“Por favor, vuelva a intentarlo”	Autentificación fallida

1.6. Sonidos durante la autentificación

“ppig”	Cuando se pulsa un botón o durante la lectura de una tarjeta. Cuando la autentificación de huella es exitosa.
“ppibig”	Autentificación fallida o entrada de usuario incorrecta.
“ppiriririck”	Esperando entrada de huella dactilar.
“ppiririck”	Autentificación exitosa o ajustes del usuario actual completados.

1.7. Señales LED

← ENCENDIDO LED: encendido o apagado

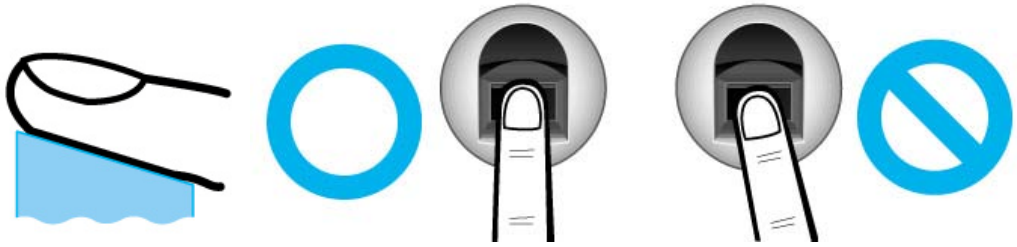
← PUERTA LED : puerta abierta o cerrada

← TARJETA LED : contacto de la tarjeta

1.8. Correcto registro de huellas dactilares y métodos de entrada

- Método correcto de registro de la huella dactilar

  Si es posible, utilice el dedo índice e introduzca el dedo como si estuviera marcando con tinta una huella dactilar. No toque sólo con la punta del dedo. La forma correcta es posicionar el centro de la huella dactilar en el centro del cristal del escáner.



- Si es posible, utilice la huella dactilar del dedo índice para la entrada. Es el más sencillo de orientar y garantizar un método de entrada estable. Utilizar el pulgar o el meñique puede dar lugar a una imagen de mala calidad.

- Compruebe si la huella dactilar es poco clara o está dañada. Una huella dactilar demasiado seca o húmeda, borrosa o con heridas es difícil de reconocer. En tal caso, use la huella dactilar de un dedo diferente para el registro.

- Precauciones a tener en cuenta debido a las condiciones de la huella dactilar del usuario.

  Una huella dactilar puede no ser utilizable o no puede ser idónea par su uso dependiendo de las condiciones de ésta.

  - Si una huella está dañada o es débil, no puede ser reconocida. Si esto ocurre, utilice una tarjeta o una clave para acceder.

  - Si el dedo está demasiado seco, sóplele durante un tiempo para asegurar un buen funcionamiento.

  - En el caso de niños, la huella dactilar puede ser demasiado pequeña o débil para utilizarla. Es necesario realizar el registro de la huella cada seis meses.

  - En caso de personas de avanzada edad, el registro puede resultar más difícil si la huella tiene un exceso de finas arrugas.

  - Si las huellas dactilares son poco claras, es conveniente registrar 2 ó 3 huellas.

  - Se recomienda registrar más de 2 huellas dactilares.

2. Introducción

2.1. Características

- Sistema de control de accesos mediante LAN

La comunicación entre la unidad y el servidor de autenticación se realiza a través de un cable UTP y el protocolo TCP / IP, por lo tanto se puede utilizar una LAN existente.

Esto garantiza una administración y supervisión basada en red, así como una fácil expansión, mayor confianza y velocidad.

- Detección automática

Proceso de autenticación simple sin ninguna introducción con las teclas, simplemente la presentación de la huella dactilar es suficiente para activar el escáner de huella.

- Autentificación sencilla usando huellas dactilares

La tecnología de autenticación de huellas dactilares evita que los usuarios olviden las contraseñas o las tarjetas o bien el robo de éstas. Es una buena forma de mejorar el nivel de seguridad.

- Alta capacidad de procesamiento del terminal y el servidor
  - Cuando se utilice un servidor no hay ninguna limitación en la información del usuario. Es posible gestionar la autentificación de más de 8.000 huellas dactilares.

- Mensajes de información
  Facilitan el proceso de autentificación debido a los mensajes de voz y en la pantalla LCD durante el reconocimiento. La luz de fondo en la pantalla LCD facilita el reconocimiento en espacios oscuros.

- Telefonillo

Fácil identificación del visitante y respuesta conveniente.

- Controles de acceso variados y flexibles

- Sin riesgo de falsificación o pérdida de llaves o tarjetas.
- Perfecto control mediante la asignación de diferentes permisos de

seguridad para cada usuario o grupo.
- Proporciona flexibilidad para la entrada y salida en un tiempo determinado.
- Bajo mantenimiento
- Sin necesidad de emitir tarjeta de visitante
-

● Aplicaciones variadas:

- Control horario
- Comida / Cafetería
- Control de acceso
- Varios modos de funcionamiento según la configuración del menú de terminal

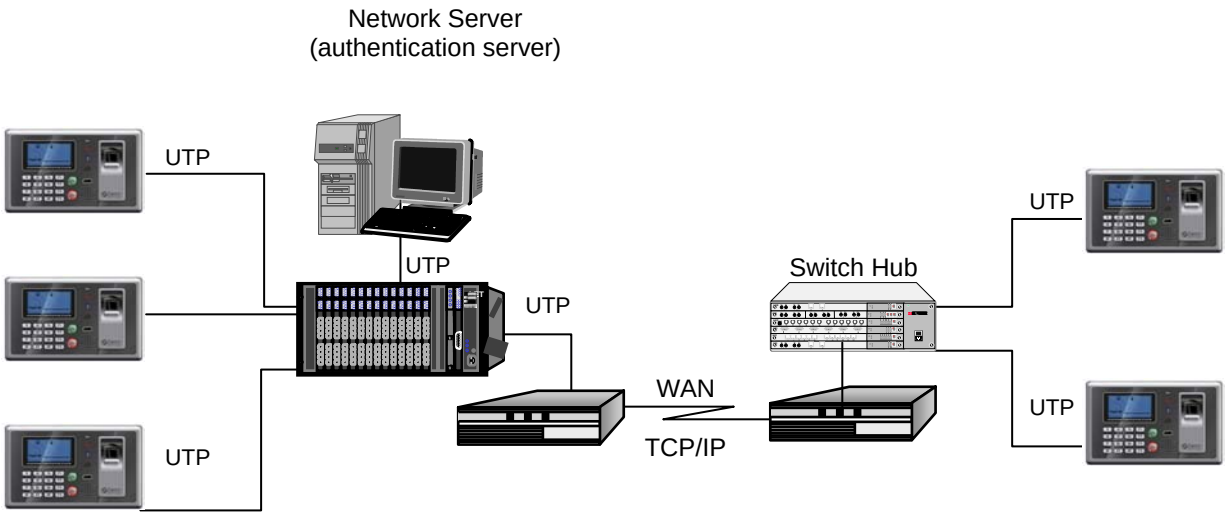
● Varios métodos de registro y autentificación
- Hay un total de 11 métodos de autentificación y registro (4 métodos si el lector de tarjetas no está instalado), por lo que es necesario seleccionar un método antes de registrar los usuarios y un administrador.

FP	Autentificación por huella dactilar
ID&PW	Registro contraseña Contraseña para autentificación después de la entrada del ID
FP|PW	Huellas dactilares y contraseña de registro Huellas dactilares o contraseña de autentificación
FP&PW	Huellas dactilares y registro de contraseña Contraseña de autentificación después de la autentificación por huella dactilar
RF	Registro de tarjeta Autentificación por tarjeta
RF|FP	Registro de tarjeta y huella dactilar Autentificación por tarjeta o huella dactilar
RF&FP	Registro de tarjeta y huella dactilar Autentificación de huella dactilar después presentar la tarjeta
RF|PW	Registro de tarjeta y contraseña Autentificación por tarjeta o contraseña
RF&PW	Registro de tarjeta y contraseña

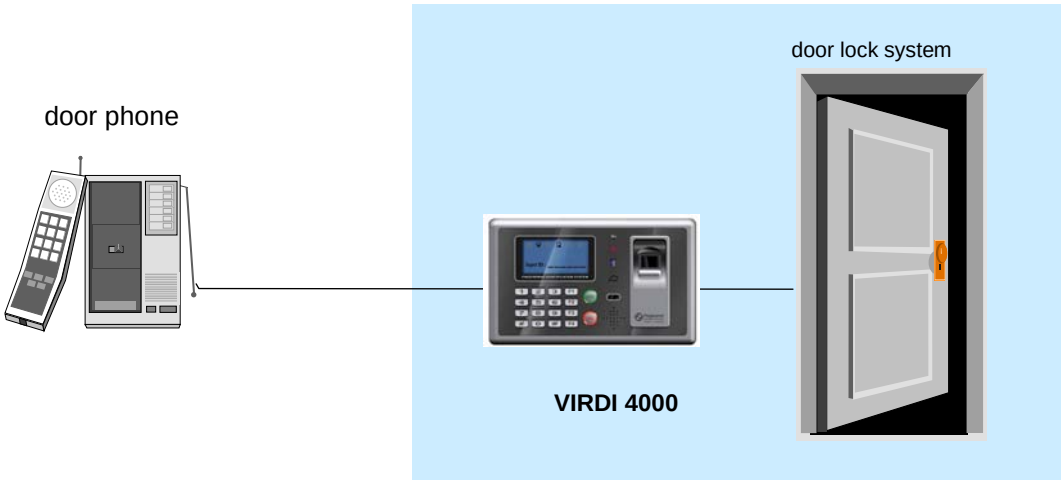
	Autentificación por contraseña después de autentificación por tarjeta
ID&FP|RF&FP	Registro de tarjeta y huella dactilar Autentificación por entrada ID y huella dactilar o autentificación por tarjeta y huella dactilar.
ID&PW|RF&PW	Registro de tarjeta y contraseña Autentificación de por contraseña y entrada ID o autentificación por contraseña y autentificación de tarjeta.

2.2. Configuración

2.2.1. Configuración de la red



2.2.2. Configuración autónoma



2.3. Especificaciones

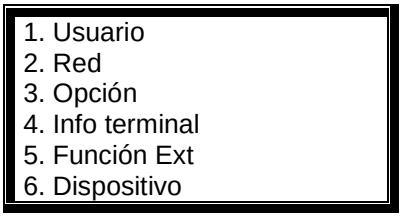
ITEM	SPEC	REMARK
CPU	32Bit RISC CPU	
MEMORIA	8M SDRAM	
	4M FLASH (Por defecto)	3,440 fingerprints
	8M FLASH (Option)	8,080 fingerprints
Sensor de huella dactilar	Optico	
Velocidad autentificación	<1 sec.	
Area escaneo / Resolución	12.9 * 15.2mm / 500 DPI	
FRR / FAR	0.1% / 0.001%	
Puerto comunicación	TCP/IP, RS-232, Wiegand	
	RS-485 (Opcion)	
Temperatura / Humedad	-10 ~ 50 / Menor de 90% RH	
LCD	128 X 64 Graphic LCD	
Area visualización	181 X 109 X 43 mm	
Transformador AC/ DC	INPUT : Universal AC 100 ~ 250V	
	OUTPUT : DC 12V (Option : DC 24V)	
	UL, CSA, CE Approved	
Opción	Lector de tarjeta RF	EM Card, 125kHz
	Lector tarjeta inteligente	A-type, 13.56MHz
	Telefonillo	

3. Configuración

3.1. Comprube el producto antes de configurarlo.

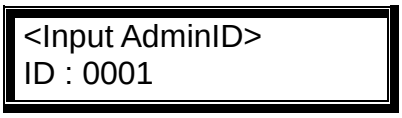
3.1.1. Menu

La siguiente pantalla aparecerá cuando presione [*] más de 2 segundos.



Presione [0] para mostrar los menus que no aparecen en la ventana LCD.

Si pulsa un número del menú (ej: 1. Usuario), aparecerá la siguiente pantalla para la autentificación del administrador:



Pulse [ENTER] después de introducir el ID de usuario, y la autentificación del administrador será procesada de acuerdo a la configuración establecida como autentificación con huella dactilar o con contraseña. Si el proceso es correcto, aparecerán los sub-menús del menú elegido.

※ La autentificación del administrador se requiere solamente una vez, por lo que todos los menús serán accesibles desde que este salga del menú por completo.

3.1.2. Cambiar configuración

Para realizar cambios, pulse la tecla [#] para borrar valores antiguos e introducir los nuevos.

Pulse [0] para visualizar los menus que no se muestren en la pantalla LCD, y elija el número correspondiente del menú.

Pulse [ENTER] para verificar configuración o pasar al siguiente ajuste.

Mantenga pulsado el botón [#] durante más de 2 segundos para cancelar el ajuste actual y pasar al menú superior.

3.1.3. Guardar configuración

Pulse el botón [#] del menú principal para guardar los ajustes.
Aparecerá la siguiente pantalla:

Save? [Y=1/N=2]:_

Pulse [1] para guardar los cambios. Para cancelar, pulse [2].

- Cuando no hay cambios para guardar, no aparecerá la ventana “Save?”, sino la pantalla inicial.
- Si no hay entradas durante cierto periodo en la pantalla de configuración, el proceso finalizará.
- Si hay cambios realizados en la configuración, aparecerá la ventana “Save?”. En caso contrario, ésta no aparecerá y se mostrará la pantalla inicial.

3.2. Configuración del menú

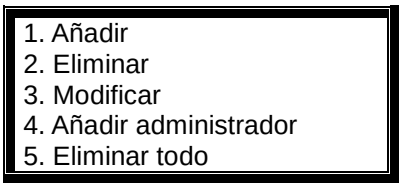
<table>
<tr><td>1. Usuario</td><td colspan="2">1. Añadir
2. Eliminar
3. Modificar
4. Añadir administrador
5. Eliminar todo</td></tr>
<tr><td>2. Red</td><td colspan="2">1) ID del terminal
2) Modo [NS/SN/NO]
3) Tipo de red [Static IP/DHCP]
4) Dirección IP
5) Máscara de subred
6) Entrada
7) Servidor IP
8) Puerto del servidor</td></tr>
<tr><td rowspan="6">3. Opción</td><td>1. Aplicación
[Entradas/ Salidas]</td><td><Aplicación>
<Entrada>
<Salida>
<Tiempo normal>
<Tecla multi-función></td></tr>
<tr><td>2. Verificacion</td><td><Mostrar Id usuario >
<Solo tarjeta>
< 1:N>
<Id usuario User>
<Verify Multi-FP></td></tr>
<tr><td>3. Set Doorlock/Cerradura</td><td><Open Duration>
<Door Monitor>
<Door Open Alarm></td></tr>
<tr><td>4. Control de sonido / Conf. Hora</td><td><Voz >
<Volumen>
<Case Open Alarm></td></tr>
<tr><td>5. Time Setting</td><td></td></tr>
<tr><td>6. Other Setting / Otros</td><td><LCD Backlight></td></tr>
<tr><td>4. Terminal Info</td><td colspan="2">Terminal ID=0001
Version=10.41.00
Application=Access
Language=ENG
Mode=NS
Network Type= Static(1)
Mac-Address=000265201111</td></tr>
</table>

	IP Address=192.168.0.3 Gateway=192.168.0.1 Subnet Mask=255.255.255.0 Server IP=192.168.0.2 Svr-Port==2201 Card Reader=None FP-Sensor=FOS02 1:1 Level=4 1:N Level=5 Max User=0 MAX FP=0 All User=0 All Admin=0 All FP=0 1:N User=0 1:N FP=0 All Log=0	
5. Funciones externas	1. Bloquear Terminal 2. Lectura de tarjeta.	
6. Dispositivo	1. Set Fn-Key	
	2. Lector de tarjeta	
	3. Sensor de huella dactilar	<Nivel 1:1 > <Nivel 1:N > <I-Capture>
	4. Wiegand	
	5. Configuración del sistema	<ID Length> <Idioma>
	6. Initialize	1. Init Config 2. Delete Log 3. Init Terminal

3.3. Usuario

3.3.1. Registro de usuario

Pulse el botón [1] del menu principal “1.Usuario”,
Aparecerá la siguiente pantalla:



Pulse [1] para registrar un usuario nuevo.

Introduzca el ID del usuario nuevo y pulse [ENTER].

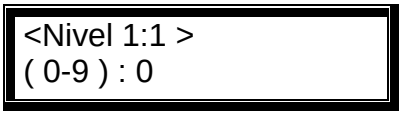
Si el ID introducido ya existe, se oirá un sonido “ppibig” y volverá al menú superior. En caso contrario, aparecerá la siguiente pantalla de selección del método de autentificación:

Pulse [0] para mostrar los menus que no aparecen en la pantalla LCD. Seleccione un método de registro de los 11 disponibles.

3.3.1.1. Registro “1. FP”

Registro con huella dactilar

◆ [ENTER] → [1] → [1] → ID de usuario [ENTER] → [1] → Nivel 1:1 [ENTER]
→ Habilitar 1:N [ENTER] → Entrada FP → ◆



Configuración recomendada: ‘0’

Se puede asignar un nivel de autentificación diferente a cada usuario.
Si está puesto a “0”, se usa el nivel de autentificación para los terminales en vez del nivel asignado a cada usuario. Cuando la verificación 1:1 en el terminal es modificada, el resto de identificaciones de usuario pasa a ‘0’.

Pulse [ENTER] para pasar a la siguiente configuración:

<Habilitar 1:N > (N=0/Y=1) : 1

El valor predeterminado es ‘1’. Se establece ‘1’ para habilitar la autentificación 1:N.

Si no hay muchos usuarios o para la comodidad de un usuario específico, se puede utilizar solamente la huella dactilar para la autentificación, sin ID.
Para la autenticación sin ID, éste se pondrá a '1 '. Para la autenticación con ID,éste se pondrá a '0 '.

Pulse [ENTER] para introducir las huellas dactilares.

<Añadir FP> Entrada huella dactilar

Oirá un sonido “ppiriririck” dos veces y la luz del sensor de huella se encenderá. Coloque el dedo en la ventana de entrada de huella y espere 2-3 segundos hasta que la luz se apague y la huella dactilar haya sido guardada.

Para introducir otra huella, retire completamente el dedo del primer reconocimiento para un mejor nivel de autentificación.
Si oye un sonido “ppiririck”, el registro es correcto. Volverá a la ventana “1.Añadir”. Si la calidad de imagen de huella no es bastante buena o no hay entrada durante 10 segundos, la luz se apagará y volverá a la ventana “1.Añadir”. En este caso oirá un sonido de error “ppibig”.

Repita los pasos anteriores 2-3 veces para completar el registro de huellas dactilares correctamente. En caso de error, se recomienda el uso de una contraseña.

3.3.1.2. Registro “2. ID&PW”

Registro de contraseña y autentificación con contraseña para el usuario

◆[ENTER] → [1] → [1] → ID de usuario [ENTER] → [2]
→ Entrada PW [ENTER] → Entrada PW [ENTER] ◆

< Entrada PW> **PW :** _ _ _ _ _ _ _ _

Entrada de contraseña. Debe contener entre 1-8 caracteres.

Pulse [ENTER] para confirmar la contraseña.

<Confirmar PW > PW : _ _ _ _ _ _ _ _

Introduzca la misma contraseña de nuevo para su verificación.

Si oye un sonido “ppiririck”, el registro se ha hecho correctamente. Si escucha un sonido diferente “ppibig”, indica que el registro no es correcto y aparecerá la ventana “1.Anadir”.

3.3.1.3. Registro “3. FP|PW”

Registro de huella dactilar y contraseña, y autentificación de huella digital o contraseña.

◆ [ENTER] → [1] → [1] → ID de usuario [ENTER] → [3] → Entrada PW [ENTER]
→ Entrada PW [ENTER] → Nivel 1:1 [ENTER] → Habilitar 1:N [ENTER] → Entrada FP → Entrada mismo FP ◆

Después del registro de huellas digitales, consulte ① Registro "1. FP", para registro de contraseña, consulte ② "2. ID y contraseña”; si escucha un sonido “ppiririck”, el registro se ha hecho correctamente. Por el contrario, si escucha “ppibig” indica un fallo en el registro y aparecerála ventana de menú “1. Añadir”.

3.3.1.4. Registro “4. FP&PW”

Registro de huella dactilar y contraseña, autentificación de huella dactilar y contraseña

◆ [ENTER] → [1] → [1] → ID de usuario [ENTER] → [4] → Entrada PW [ENTER]
→ Entrada PW [ENTER] → Nivel 1:1 [ENTER] → Habilitar 1:N [ENTER]
→ IEntrada FP → Entrada mismo FP ◆

Después del registro de huellas dactilares, consulte ① registro "1.FP", para registro de contraseña, consulte ② "2. ID y contraseña" registro.

3.3.1.5. Registro “5. RF”

Registro y autentificación de Tarjeta

◆[ENTER] → [1] → [1] → ID de usuario [ENTER] → [5] → Coloque la tarjeta ◆

<Añadir tarjeta> Coloque la tarjeta

Para cancelar el registro, pulse el botón [#].

Si el usuario coloca la tarjeta cerca de la unidad, se oirá un sonido “ppiririck” (registro correcto) y aparecerá la ventana“1. Añadir”.

3.3.1.6.Registro “6. RF|FP”

Registro de huella dactilar o tarjeta, autentificación de huella dactilar o tarjeta

◆[ENTER] → [1] → [1] → ID de usuario [ENTER] → [6] → Coloque la tarjeta → Nivel 1:1 [ENTER] → Habilitar 1:N [ENTER] → Entrada FP → Entrada mismo FP ◆

Después del registro de tarjeta, consulte ⑤ Registro “5. RF” ", para registro de huella dactilar, consulte ① Registro“1. FP” ".

.

3.3.1.7. Registro“7. RF&FP”

Registro de huella dactilar y tarjeta, autentificación de tarjeta y huella dactilar

◆[ENTER] → [1] → [1] → ID de usuario [ENTER] → [7] → Coloque la tarjeta → Nivel 1:1 [ENTER] → Entrada FP → Entrada mismo FP ◆

Despues del registro de tarjeta, consulte⑤ “Registro 5. RF”, para registro de huella dactilar, consulte ① “Registro 1. FP”.

3.3.1.8. Registro “8. RF|PW”

Registro de tarjeta o contraseña, autentificación de tarjeta o contraseña

◆[ENTER] → [1] → [1] → ID de usuario [ENTER] → [8] → Coloque su tarjeta → Entrada PW [ENTER] → Entrada mismo PW ◆

Despues del registro de tarjeta, consulte ⑤ “Registro 5. RF”, para registro de contraseña, consulte ② “Registro 2. ID&PW”.

3.3.1.9. Registro “9. RF&PW”

Registro de tarjeta y contraseña, autentificación de tarjeta y contraseña

◆[ENTER] → [1] → [1] → ID de usuario [ENTER] → [9] [1] → Coloque la tarjeta → Entrada PW [ENTER] → Entrada mismo PW [ENTER] ◆

Despues del registro de tarjeta, consulte ⑤ “Re5. RF”), para registro de contraseña, consulte ② Registro “2. ID&PW” .

3.3.1.10. Registro “10. ID&FP|RF&FP”

Registro de ID y huella dactilar o autentificación de tarjeta y huella dactilar.

.

◆[ENTER] → [1] → [1] → ID de usuario [ENTER] → [9] [2] → Coloque la tarjeta → Nivel 1:1 [ENTER] → Entrada FP → Entrada mismo FP ◆

En este caso, se utiliza una tarjeta en lugar del ID para la autentificación. Esto es útil para los usuarios que tienen dificultades para introducir su ID.

Despues del registro de tarjeta, consulte Registro “5. RF” , para Registro de huella dactilar consulte Registro “1. FP”.

3.3.1.11. “11. Registro ID&PW|RF&PW”

Registro de ID y contraseña o autentificación de tarjeta y contraseña

◆[ENTER] → [1] → [1] → ID de usuario [ENTER] → [9][3] → Coloque la tarjeta → IEntrada PW [ENTER] → Entrada mismo PW [ENTER] ◆

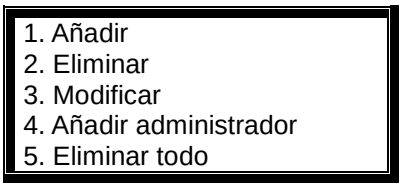
En este caso, se usa el ID en lugar de la tarjeta. Esto es útil para los usuarios que tienen dificultades para introducir su ID.

Despues del registro de tarjeta, consulte Registro “5. RF”, para el registro de contraseña consulte Registro“2. ID&PW”.

3.3.2. Eliminar usuario

◆[ENTER] → [1] → [2] → ID de usuario [ENTER] ◆

En el menu principal, pulse [1] para seleccionar “1.Usuario”. Aparecerá la siguiente ventana:



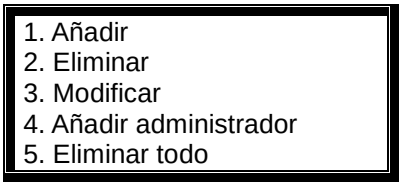
Para eliminar un usuario pulse [2].

Después de introducir el ID de usuario que quiere eliminar, pulse [ENTER] y toda la información del usuario será borrada, oirá el sonido “ppiririck”. Sin embargo, esta información todavía quedará almacenada en el servidor. Para eliminarla completamente, los datos del servidor también tendrán que ser borrados.
Si se introduce un ID de usuario no registrado, “2. Eliminar” aparecerá junto con un sonido “ppibig”.
Se debe tener precaución cuando se elimina un usuario o un administrador. El usuario recién registrado en la unidad (no en el servidor) no se puede recuperar, por lo que se requiere un cuidado especial.

3.3.3. Modificar un usuario

◆[ENTER] → [1] → [3] → ID de usuario [ENTER] → Seleccione Menu → cambie el valor ◆

En el menu principal, pulse [1] para seleccionar “1. Usuario”. Aparecerá la siguiente pantalla:



Para modificar un usuario pulse [3].

Introduzca el ID del usuario que quiera modificar, y pulse [ENTER].

A la hora de cambiar el ID de un usuario, es irrelevante que sea o no administrador.
Si se introduce un usuario no registrado (o administrador), se oirá un sonido “ppibig” y aparecerá el menú “1. Añadir”.

3.3.3.1. “1. FP” Usuario

Si la huella dactilar de un usuario ya está registrada, es posible un registro cambiando el nivel de identificación o una huella dactilar adicional.

.

1. Nivel 1:1 2. Añadir FP

Para cambiar el nivel de autentificación, pulse [1]. Para añadir una huella dactilar a su correspondiente ID, pulse [2].

※ Es posible añadir un máximo de 5 huellas dactilares a un ID. Si intenta agregar más de éstas oirá un sonido “ppibig” al pulsar la tecla [2].

[1] Cuando selecciona el cambio de nivel de verificación:

< 1:1 Level> (0-9) : 0

Configuración recomendada: ‘0’

Para cambiar los ajustes, introduzca los ajustes nuevos.

[2] Cuando selecciona el registro de huellas adicionales

<Añadir FP> Entrada FP

Escuchará un sonido “ppiriririck” dos veces y la luz del sensor de huellas se encenderá. Coloque el dedo sobre el sensor y espere durante 2- 3 segundos hasta que la luz se apague y la huella quede guardada.

Si escucha un sonido “ppiririck”, el registro se ha completado correctamente. Volverá a la pantalla “1.Añadir ”. Si la imagen de la huella dactilar no es muy visible o no hay entrada de huella durante 10 segundos, volverá a la pantalla “1. Añadir” y oirá un sonido de error “ppibig”.

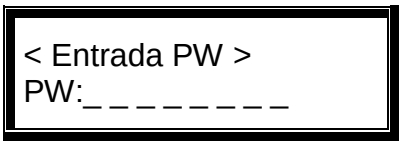
3.3.3.2. “2.ID&PW”

Cuando un usuario quiere cambiar su contraseña:

1. Modificar PW

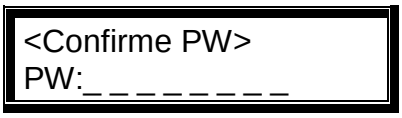
Para cambiar la contrasela, pulse [1]. Para cancelar, pulse [#].

Pulse [1] para cambiar la contraseña:



Entrada contraseña. Ésta deberá tener entre 1-8 caracteres.

Pulse [ENTER] para introducir la contraseña.

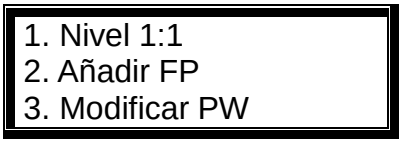


Confirme su contraseña.

Pulse [ENTER] para confirmar.

Si el cambio de contraseña se realiza correctamente, oirá un sonido “ppiririck”. Por el contrario, si es incorrecto oirá un sonido “ppibig” y aparecerá la pantalla del menú “1. Añadir”.

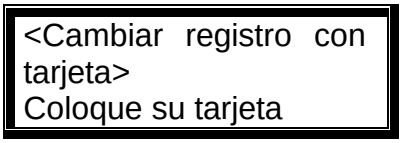
3.3.3.3. “3.FP|PW”, “4.FP&PW” Usuario



Pulse [1] para cambiar el nivel 1:1 (refer “3.3.3.1”)
Pulse [2] para registrar huellas adicionales (refer “3.3.3.1”)
Pulse [3] para cambiar contraseñas (refer “3.3.3.2”).
Para cancelar, pulse [CLR].

3.3.3.4. “5.RF” Usuario

Para cambiar el registro con la tarjeta, pulse [1].
Para cancelar, pulse [#].



Si un usuario coloca la tarjeta cerca del terminal se escuchará un sonido “ppiririck” (modificación realizada correctamente) y aparecerá la pantalla del menú “1. Añadir”.

3.3.3.5. Usuario “6.RF|FP”,”7.RF&FP”,”92.ID&FP|RF&FP”

1. Nivel 1:1 2. Añadir FP 3.Cambiar registro tarjeta

Pulse [0] para mostrar los menus que no aparecen en la pantalla LCD. Para cancelar, pulse[#].

Pulse [1] para cambiar el nivel 1:1 (refer “3.3.3.1”)
Pulse [2] para registrar huellas adicionales (refer “3.3.3.1”)
Pulse [3] para cambiar el registro de tarjeta (refer “3.3.3.2”).
Para cancelar, pulse [CLR].

3.3.3.6. Usuario “8.RF|PW”,”91.RF&PW”,”93.ID&PW|RF&PW”

1. Modificar PW 2. Cambiar registro tarjeta

Pulse [1] para cambiar la contraseña (refer “3.3.3.2”).
Pulse [2] para cambiar el registro con tarjeta (refer “3.3.3.4”).
Para cancelar, pulse [#].

3.3.4. Registro del administrador

◆[ENTER] → [1] → [4] → Admin ID [ENTER] ◆

En el menu principal, pulse [1] para seleccionar “1.Usuario”, y seleccione [0]. Aparcerá la siguiente pantalla:

1. Añadir 2. Eliminar 3. Modificar 4. Añadir administrador 5. Eliminar todo

Para registrar un administrador, pulse [4].

Admin ID [NEW] ID : _ _ _ _

Introduzca el ID del administrador y pulse [ENTER].

※El proceso de registro para el administrador es el mismo que para cualquier ususario.

Solamente un administrador puede cambiar el funcionamiento del terminal y registrar/modificar/eliminar información de usuarios, por lo que se requiere especial cuidado a la hora de registrar un usuario.

3.3.5. Eliminar usuarios

◆[ENTER] → [1] → [5] ◆

En el menu principal, pulse [1] y seleccione “1. Usuario”.
Pulse [0] y aparecerá la siguiente pantalla:

1. Añadir 2. Eliminar 3. Modificar 4. Añadir administrador 5. Eliminar todo

Para borrar todos los usuarios, pulse [5].

Eliminar todo? [Y=1/N=2] : _

Para eliminar todos los usuarios pulse [1].Para cancelar, pulse [2].

Se require un cuidado especial, ya que con esta operación se borran todas las cuentas de usuario, incluyendo la del administrador.
Cuando la operación es correcta, se escuchará un sonido “ppiririck” y aparecerá la ventana del menú “1. Añadir” .

3.4. Configuración de la red

En el menu principal, pulse [2], seleccione “2.Network” para visualizar la siguiente pantalla. Cuando ha escogido el ajuste, pulse [ENTER] para pasar a la siguiente configuración.

3.4.1. Número ID del terminal

◆[ENTER] → [2] ◆

```
< Terminal ID >
ID : 00000001
```

El número ID del terminal únicamente identifica al terminal en el programa servidor de red. El valor por defecto es ‘00000001’. Por cada terminal en el servidor de red se debe establecer un número diferente. Este valor debe tener de 1-8 dígitos de longitud.

Si el ID del terminal es ‘1000’, introduzca [1][0][0][0]. Si es ‘0001’, introduzca solamente [1]. Pulse [ENTER] para pasar al siguiente ajuste.

3.4.2. Modos de conexión [NS / SN / NO]

```
Modo [ NS / SN / NO ]
( 0-2 ) : 0
```

NS modo: ‘0’, SN modo: ‘1’,
NO modo: ‘2’

Esto define el metodo de autentificación entre el terminal y el servidor de red. El valor por defecto es ‘0’ (NS). Cada método de autentificación se describe a continuación:

- NS modo: seleccione [0]. Cuando hay una conexión con el servidor, la autentificación se realiza a través del servidor. Si no, se realiza a través del terminal.

- SN mode: seleccione [1]. Aunque haya una conexión activa con el servidor, la autentificación se realiza a través del terminal y el resultado se envía al servidor en tiempo real. Sin embargo, en el caso de la autentificación 1:1, si el ID de usuario introducido no se ha registrado en el servidor, la autentificación se realiza a través del servidor.

- NO mode: seleccione [2]. Aunque un usuario se haya registrado en el terminal, la autentificación se realiza a través del servidor.

Dependiendo del número de terminales, número de usuarios o condiciones de la red, los modos se pueden utilizar de forma flexible. Cuando hay más de 10 terminales conectados al servidor para la autentificación simultánea o hay problemas de red frecuentes, se recomienda utilizar la autentificación SN (ajuste '1').

Pulse [ENTER] para pasar al siguiente ajuste.

3.4.3. Configuración del método de conexión

◆[ENTER] → [2] → [ENTER] → [ENTER] ◆

Tipo de red: 0 0:Estático 1:DHCP

Pulse [0] para IP Estático.
Pulse [1] para DHCP.

El valor por defecto es '0' (IP Estático). Si un IP fijo se asigna a la unidad en una red, pulse [0]. Si hay un servidor DHCP en la red al que está conectada la unidad, pulse [1].

Pulse [ENTER] para pasar al siguiente ajuste.

※ For Static IP (0), refer to 3.4.4. IP address, 3.4.5. Subnet mask, and 3.4.6. Gateway. For DHCP, skip those sections.

3.4.4. Configuración de la direccion IP

< Dirección IP > 192.168. 0. 3

Pulse [#] para borrar el IP antigüo e introducir el nuevo.

Si la dirección de IP es '210.98.100.50', introdúzcalo de la siguiente forma:

[2] [1] [0] [9] [8] [*] [1] [0] [0] [5] [0]

Pulse [ENTER] para pasar al siguiente ajuste.

※ IP 설정 시 숫자만 입력하며 두자리 이하의 숫자를 입력 후 다음 칸으로 이동 시 [*]버튼을 누릅니다.

3.4.5. Configuración de la mascara de subred

<Mascara de subred> 255.255.255. 0

Pulse [#] para eliminar el valor antigüo e introducir el nuevo.

Si el número es ‘255.255.255.0’, introdúzcalo de la siguiente manera:

[2] [5] [5] [2] [5] [5] [2] [5] [5] [0]

Pulse [ENTER] para pasar al siguiente ajuste.

3.4.6. Puerta de enlace

<Gateway> 192.168. 0. 1

Pulse [#] para eliminar el valor antigüo e introducir el nuevo.

Si la dirección de IP de entrada es ‘210.98.100.1’, introduzcalo de la siguiente forma:

[2] [1] [0] [9] [8] [*] [1] [0] [0] [1]

Pulse [ENTER] para pasar al siguiente ajuste.

3.4.7. IP del Servidor

< Server IP > 192.168. 0. 2

Pulse [#] para eliminar el valor antigüo e introducir el nuevo.

Si la dirección del servidor es “210.98.100.121”, introdúzcalo de la siguiente forma:

[2] [1] [0] [9] [8] [*] [1] [0] [0] [1] [2] [1]

Pulse [ENTER] para pasar al siguiente ajuste.

3.4.8. Puerto del servidor

< Server port > Num : 9870

Pulse [#] para eliminar el valor antigüo e introducir el nuevo.

Como número de autentificación del puerto, el valor por defecto es ‘2201’. Es

preciso tener un cuidado especial al cambiar este número porque el número correspondiente en el servidor también debería ser cambiado.

Si el número del puerto del servidor es ‘9870’, introdúzcalo de la siguiente forma:

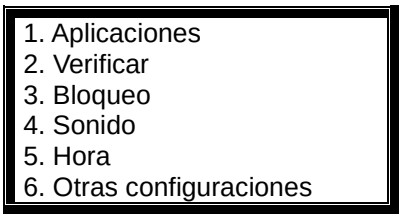
[9] [8] [7] [0]

Una vez que la configuración de red se haya completado, pulse [ENTER] para volver al menú principal.

3.5. Ajustes

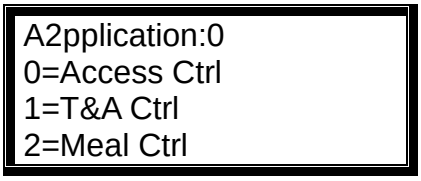
3.5.1. Application mode settings

En el menu principal, pulse [3] y seleccione “3. Opciones”. Aparecerá la siguiente pantalla:



Para establecer el modo de funcionamiento básico del terminal, pulse [1].

◆[ENTER] → [3] → [1] ◆



El valor por defecto es ‘0’ (Access Ctrl).

Para un sencillo control de acceso, se establece '0 '; para el control horario, se pone a '1 '.
Para comida se pone 2.
Pulse [ENTER] para pasar a la configuración detallada de cada modo de funcionamiento.

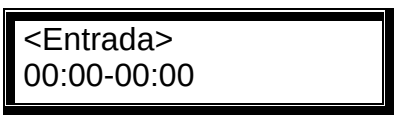
3.5.1.1. [0]: Control de acceso

No hay ajustes más detallados. Volverá al menú superior.

3.5.1.2. [1]: Horarios control de presencia

Si <multi-key authentication> se establece como el modo de funcionamiento, más de 40 modos secundarios pueden ser definidos.

El tiempo predeterminado se puede ajustar a Entrada / Descanso / Fin Descanso / Salida. Después de la autentificación, el modo de pantalla del terminal se puede cambiar automáticamente al modo de funcionamiento programado. Si la tecla multifunción se establece en funcionamiento, pueden ser definidos mas de 40 modos secundarios.



Si no es necesario establecer horario de entrada, ajuste el horario como ‘00:00-00:00’.

Para cambiar el horario de entrada de ‘00:00~00:00’ a ‘06:00~09:59’, pulse

[CLR] y eliminará los ajustes de horarios existentes. Introduzca el nuevo horario de la siguiente forma: [0][6][0][0][0][9][5][9].

Siempre y cuando no se presione ningún botón durante el funcionamiento, el terminal funcionará en modo “Entrada”. Incluso si realiza el trabajo fuera, la autentificación es correcta.

Despues de configurar el horario de <Entrada >, ajuste el horario de <Salida> y <Descanso y Fin Descanso> de la misma forma. Los modos no deben superponerse.

Ej.)Entrada:06:00~09:59, Salida:17:00~22:00, Tiempo Normal:10:00~16:59

< Entrada >	< Salida >	< Tiempo Normal >
06:00~09:59	17:00~22:00	10:00~16:59

Después de ajustar el tiempo real, pulse [ENTER] par ver el menu de ajustes “Multi Fn-key”, el cual permite más de 5 modos de trabajo.

<Multi Fn-key>
1=F1:X 2=F2:X
3=F3:X 4=F4:X

Valor por defecto: todos ‘X’

Este menu resulta útil cuando son necesarios más de 5 modos de trabajo.
- Ajuste X: cada tecla de función representa un modo de trabajo: F1=Entrada, F2=Salida, F3=Descanso, y F4= Fin descanso. Cuando se pulsa una tecla de función, el modo de autenticación cambia al modo de trabajo correspondiente.
- Ajuste O: un modo se define por la combinación de una tecla de función y una tecla numérica, tales como “F3+1”.

(Ej.) ☒
Si el valor es 1 = F1: X 2 = F2: X 3 = F3: X 4 = F4: O, 14 modos de trabajo diferentes se pueden definir de acuerdo a la entrada del usuario, tal como [ENTER]: [F1]: Entrada al trabajo, [F2]: Final jornada laboral, [F3]: comienzo descanso, y [F4] final descanso.

El ajuste O / X se puede cambiar pulsando la tecla numérica correspondiente. Una vez completada la configuración, pulse [ENTER] para ir al menú superior.

3.5.1.3. [2] Horarios comidas

<Desayuno>
00:00-00:00

Si no es necesario establecer horario de desayuno ajuste el horario como ’00:00-00:00’

조식시간을 설정하는 것으로 설정된 시간대에는 무조건 조식으로 인증됩니다.
조식시간 설정이 끝난 후 동일한 방법으로 <Lunch>, <Dinner>, <Supper>,

<Snack>을 차례로 설정하며, 사용하지 않는 식사는 00:00-00:00으로 설정합니다.

각각의 시간대는 서로 겹치지 않도록 설정하고 설정된 시간대 내에서 각 사용자는 한번씩만 인증이 가능하며, 사용자가 꼭 중복인증을 해야 하는 경우에는 [ENTER]키를 누른 상태에서 지문 또는 카드를 대서 인증할 수 있습니다.

식수시간대로 설정되지 않은 시간에 단말은 “잠금 설정!” 메시지가 디스플레이 되며 단말기 잠금 시와 동일하게 메뉴모드로의 진입을 제외한 모든 입력이 차단됩니다.

<Snack>까지 모두 설정한 후 [ENT]키를 입력하면 아래와 같이 <Without Limit>여부를 설정하는 메뉴가 나옵니다.

<Sin Limite> (N=0/Y=1):0

Valor por defecto: ‘0’

중복인증제한을 하는 경우 ‘0’ 으로 설정하여 식수설정시간에 한 사용자가 한번만 인증 할수 있으며, 중복인증을 하려면 ‘F4’ 키와 함께 사용하여 인증시 가능하다.
중복인증제한을 하지 않으려면 ‘1’ 로 설정하여 인증시 제한을 주지 않는다.

설정후 [ENT]키를 입력하면 아래와 같이 <Ticket Printer> 를 설정하는 메뉴가 나옵니다.

Imprimir Ticket (N=0/Y=1):0

Valor por defecto: ‘0’

식권프린터 연동여부를 설정하는 것으로 ‘1’로 설정 시 인증이 성공하면 RS232-1포트에 연결된 프린터로 식권인쇄명령을 보냅니다.
이때 사용되는 프린터는 “SRP-350”모델이며 단말기ID, 사용자ID, 일자, 식사종류별 식권일련번호, 식사종류 등이 인쇄됩니다.

3.5.2. Ajustes de métodos de autentificación

En el menu principal, pulse [3] y selecciones “3. Opciones”. Aparecerá la siguiente pantalla:

1. Aplicaciones 2. Verificar 3. Bloqueo

Para configurar el método de autenticación predeterminado, presione [2].

4. Sonido 5. Hora 6.Otras configuraciones

3.5.2.1. Ajustes para la visualización de ID cuando la autentificación es correcta

◆[ENTER] → [3] → [2] ◆

<Mostrar ID de usuario> (N=0/Y=1):0

Valor por defecto: ‘0’

Si se ajusta a la configuración por defecto [0], sólo se muestra el mensaje "Correcto". Si se ajusta en [1] y la autentificación es correcta, se muestra en la pantalla LCD el ID del usuario: (Ej.) OK! <0001>

Pulse [ENTER] para pasar la siguiente ajuste.

3.5.2.2. Ajustes para la autentificación de tarjetas

◆[ENTER] → [3] → [2] → [ENTER] ◆

<Only Card> (N=0/Y=1):0

Valor por defecto: ‘0’

Incluso para un usuario que esté registrado con tarjeta y PW / tarjeta y huella dactilar, cuando esta opción se establece en '1 ', sólo tiene que utilizar la tarjeta.

Esta opción se utiliza generalmente cuando hay terminales instalados en la puerta de entrada del edificio donde la entrada/salida de usuarios es frecuente y el nivel de seguridad es relativamente bajo.

Pulse [ENTER] para pasar al siguiente ajuste.

3.5.2.3. Ajustes de autentificación 1:N

◆[ENTER] → [3] → [2] → [ENTER] → [ENTER] ◆

<Habilitar 1:N> (N=0/Y=1):0

Valor por defecto: ‘1’

Esto permite la autentificación de huellas digitales sin un ID de usuario o tarjeta. Incluso si un usuario se registra para ser autentificado con el método 1:N, sólo se permite la autenticación de 1:1 si el terminal se pone a '0 '.

Si se requiere una entrada ID o autenticación de huellas digitales después de entrada de tarjeta (cuando la entrada de la tarjeta reemplaza la entrada ID), debería fijarse a '0'.

Ajustes detallados para 1: N autenticación:

①Cuando la autentificación 1:N se pone a ‘1’

<User ID Group> (N=0/Y=1):0

Valor predeterminado: ‘0’

Tome los primeros dígitos del ID como un grupo para la autenticación, por lo que el modo 1: N se puede procesar mucho más rápido cuando hay más de 1.000 usuarios registrados.

Si se pone a '1 ', la autentificación de huellas digitales se realiza para usuarios empezando con el ID introducido. Si se pone a '0 ', tome los números introducidos como ID de usuario; las huellas dactilares del usuario y la autentificación 1:1 para el correspondiente ID.

Ej.) Cuando un ID de usuario es un número de 4 dígitos y '12 'se introduce para la autenticación, si se pone a '1', la autentificación 1:N se realiza para los ID de usuarios entre '1200 '~ '1299'. Si se ajusta a '0 ', la autenticación 1:1 se realiza para los 12 ID de usuarios con huella dactilar.

<Blocking Time> (0-86400):00000

Valor por defecto: ‘00000’

**********¿?¿?¿?

Para una autentificación exitosa, todas las huellas dactilares registradas

serán autentificadas después de la entrada ID (o tarjeta).

Se utiliza cuando se requiere un alto nivel de seguridad para zonas especiales. Si un usuario de 'ID 0001' tiene 3 huellas dactilares registradas en la unidad, los 3 huellas digitales serán autenticados después de la entrada ID.

La secuencia de autenticación para las 3 huellas digitales no importa en este caso, pero la autenticación falla si una sola huella digital no se autentifica correctamente.

Una vez que haya completado el ajuste, pulse [ENTER] para ir al menú superior.

3.5.3. Puerta / Cerradura

En el menu principal, pulse [3] y seleccione “3. Opciones”. Aparecerá la siguiente pantalla:

1. Aplicaciones 2. Verificar 3. Bloqueo/Cerradura 4. Sonido 5. Hora 6.Otras configuraciones

Pulse [3] para ajustes de puerta.

3.5.3.1. Door opening time settings

◆[ENTER] → [3] → [3] ◆

<Tiempo Apertura> (00-30):03

Valor por defecto: ‘03’ (unit: sec.)

For the dead bolt type or auto door, this time is not effective.
Esto se utiliza para ajustar el tiempo de apertura de la puerta después de una correcta autenticación. For the strike type, this means the door opening time. No es eficaz para puertas automáticas o con cerrojo.

Si está puesto a ‘00’, la puerta está fuera del control, por lo que se puede fijar a '00 'sólo para el periodo de tiempo de entrada / salida.

Para pasar al siguiente ajuste, pulse [ENTER].

3.5.3.2. Estado de la puerta

◆[ENTER] → [3] → [3] → [ENTER] ◆

<Estado Puerta> [0/1=NO/2=NC]:0

Valor por defecto: ‘0’

- ‘0’: NW – sin verificación
- ‘1’: NO – Puertas automáticas o con cerradura
  (El bloqueo está activado cuando la puerta está cerrada)
- ‘2’: NC - Strike Type
  (El bloqueo está desactivado cuando la puerta está cerrada)

Cuando se establece a '1 'o '2', la condición de puerta conectada al terminal se envía al servidor periódicamente.

Pulse [ENTER] para pasar al siguiente ajuste.

3.5.4. Volumen

En el menu principal, pulse [3] y seleccione “3. Opciones”. Aparecerá la siguiente pantalla:

1. Aplicaciones 2. Verificar 3. Bloqueo 4. Sonido 5. Hora 6.Otras configuraciones

Pulse [4] para configurar el volumen.

3.5.4.1. Ajustes de voz

<Voice Volume> (N=0/Y=1):1

Valor predeterminado: ‘0’

Para ajustar la información de voz, ajustelo a '1 '. Si no es así, póngalo en '0 '. Pulse [ENTER] para pasar al siguiente ajuste.

3.5.4.2. Ajustes de sonidos

<Beeper volume> (0-2):1

Valor por defecto: ‘1’

Controla el volumen de sonidos del terminal. Si se establece a '0 ', no hay sonidos. '1 'equivale a un volumen bajo, y '2' a un volumen alto.

Pulse [ENTER] para pasar al siguiente ajuste.

3.5.4.3. Case open alarm settings

<Conf. Alarma> (N=0/Y=1):1

Valor por defecto: ‘1’

Si el terminal está dañado o abierto, sonará una alarma. Funciona sólo cuando está instalado el sensor de caso abierto.

Pulse [ENTER] para pasar al siguiente ajuste.

3.5.5. Hora actual

◆[ENTER] → [3] → [5] ◆

En el menu principal, pulse [3] y seleccione “3. Opciones”. Pulse [5] y aparecerá la siguiente pantalla:

<Time Setting> 20060401211806

Esto es para la hora actual terminal. El ejemplo anterior representa el año 2006, mes 04, día 01, hora 21, min. 18 y s. 06. Para cambiarlo, borre los números con el botón [#] antes de añadir los nuevos.

Pulse [ENTER] para comprobar que la hora actual se actualiza y pasar al menú superior.

3.5.6. Otros ajustes

En el menu principal, pulse [3] y seleccione “3.Opciones”. Pulse [6] y aparecerá la siguiente pantalla:

1. Aplicaciones 2. Verificar 3. Bloqueo 4. Sonido 5. Hora 6.Otras configuraciones

Pulse [6] para otros ajustes.

3.5.6.1. Pantalla LCD

◆[ENTER] → [3] → [6] ◆

<LCD Backlight> (0=Off/1=On):

Valor por defecto : ‘0’

Este ajuste es para activar / desactivar la luz de la pantalla LCD.

Si se ajusta a la configuración por defecto [0], la luz de fondo de la pantalla LCD normalmente está apagada. Sólo en los casos en que un usuario opera con el teclado o tarjeta, la luz de fondo se enciende y se realiza la operación de trabajo. Ésta se apagará en 10 segundos.

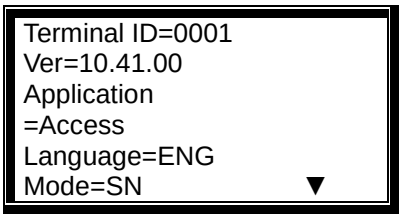
Si se ajusta a ‘1’, la luz siempre permanecerá encendida.

Pulse [ENTER] para pasar al siguiente ajuste.

3.6. Información del terminal

◆[ENTER] → [4] ◆

En el menu principal, pulse [4] y seleccione “4.Informacion del terminal”. Aparecerá la siguiente pantalla, donde se mostrarán todos los ajustes de entorno del terminal:



Pulse [0] para desplazarse hacia arriba o abajo de la pantalla.

Terminal ID	Terminal ID
Version	Terminal firmware version
Application	Terminal application mode (Access/T&A)
Language	Language for text and voice of the LCD screen
Mode	Connection mode between terminal and network server
Network type	Network connection type (fixed IP/variable IP)
Mac Address	Terminal Ethernet hardware address
IP address	Terminal IP address
Gateway	Terminal Gateway address
Subnet mask	Terminal Subnet Mask address
Server IP	IP address of network server connected to the terminal
Svr-port	Port number of network server program
Card Reader	Connected card reader type
FP-Sensor	Connected fingerprint sensor type
1:1 Level	Identification level for 1:1 authentication
1:N Level	Identification level for 1:N authentication
Max User	Max. number of users registered to a terminal
Max FP	Max. number of fingerprints registered to a terminal. For example, if there are 100 registered users and two fingerprints are registered for each user, then there is a total of 200 fingerprints registered
All User	Number of current users registered to a terminal including administrators
All Admin	Number of administrators registered to a terminal

All FP	Number of fingerprints currently registered to a terminal
1:N User	Number of users for 1:N authentication
1:N FP	Number of fingerprints for 1:N authentication
All Log	Authentication records stored in a terminal

3.7. Funciones ampliadas

En el menu principal, pulse [5] para seleccionar “5.Funciones extendidas”. Aparecerá la siguiente pantalla:

```
1. Bloqueo del terminal
2. Leer tarjeta
```

3.7.1. Ajustes de bloqueo del terminal

◆[ENTER] → [5] → [1] ◆

```
<Bloqueado>
(N=0/Y=1):0
```

Valor por defecto ‘0’: terminal lock clear
‘1’: terminal lock set

Un administrador puede configurar directamente el bloqueo para el terminal. Si se ajusta a '1 ', el terminal está bloqueado y nadie puede cruzar la puerta hasta que el administrador lo desbloquee.

※ Para esta función, el administrador deberá verificarse en las opciones del terminal del programa del servidor.

Una vez completado el ajuste, pulse [ENTER] para ir al menú superior.

3.7.2. Lectura de tarjeta

◆[ENTER] → [5] → [2] ◆

```
Coloque su tarjeta
```

Como una función auxiliar, independientemente de la configuración del entorno de terminal, un

terminal con lector de tarjetas puede leer el número de tarjeta para registrarla en el servidor.

Cuando el terminal lee la tarjeta, el número de ésta se visualiza en la pantalla LCD.

Para salir del lector de tarjeta, pulse [CLR]. Se desplazará al menú superior.

3.8. Configuración del dispositivo

En el menu principal, pulse [6] y seleccione “6. Dispositivo”. Aparecerá la siguiente pantalla solicitando la contraseña para éstos ajustes:

Se trata de una opción que no es necesario cambiar después de la instalación, por lo que se recomienda no hacerlo excepto cuando es realmente necesario.

<Entrada PW>
PW:

Esta contraseña de ajustes es sólo para información del usuario, por lo que no puede cambiarse.

Introduzca “084265” como contraseña de ajustes y pulse [ENTER] para ver las opciones de configuración detalladas.

3.8.1. Teclas de función

◆[ENTER] → [6] → ‘084265’ [ENTER] → [1] ◆

<Key On/Off>
1=F1:0 2=F2:0
3=F3:0 4=F4:0
5=Ent:O 6=FP:O

Valor por defecto: todos ‘O’

Esta opción es para activar / desactivar las teclas de función. 'O' es 'permitir' y 'X' es 'desactivar'. Cada vez que se pulsa una tecla de función, se cambia entre O / X.

1equivale a [F1], 2 a [F2], 3 a [F3], 4 a [F4], 5 a [ENTER], y 6 para la detección automatica del sensor de huellas.

Si F1 se convierte en X pulsando [1], no se puede cambiar al modo de entrada aunque se pulse [F1].

Además, si sólo se establece [F1] o [F2] en 'O', el terminal se puede utilizar en cualquiera de los dos siempre en entrada o modo de salir.

Pulse [ENTER] para pasar al siguiente ajuste.

3.8.2. Lector de tarjetas

◆[ENTER] → [6] → ‘084265’ [ENTER] → [2] ◆

Lector Tarjeta:0 0=Non 1=RF 2=SC 3=Wiegand 4=SC1 5=Ext

Valor por defecto: ‘0’

Estos son los ajustes para el lector de tarjetas conectado a un terminal. Se pondrá a '0 ', excepto en los siguientes casos:

- ‘0’: no hay lector de tarjetas
- ‘1’: se instala un lector de tarjeta RF de baja frecuencia
- ‘2’: se instala un lector de tarjetas inteligentes de alta frecuancia
- ‘3’: Se instala un lector de tarjetas de tipo Wiegand (ej.: HID...)
- ‘4’: Se instala una nueva versión del lector inteligente de RF
- ‘5’: Se instala un lector de tarjetas extermo

Si se establece un número que no sea 0 y [F1] ~ [F4] o se presiona [ENTER], sólo cambia el modo de autentificación y el modo 1:N de huellas digitales no se realiza. Sin embargo, la autentificación 1: N se realiza sólo para la detección automática.

Una vez que haya completado el ajuste, pulse [ENTER] para ir al menú superior.

3.8.3. Sensor de huellas dactilares

3.8.3.1. Verificación 1:1

◆[ENTER] → [6] → ‘084265’ [ENTER] → [3] ◆

1:1 Nivel (1-9):4

Valor predeterminado: ‘4’

Establece el nivel de concordancia entre la entrada de las huellas dactilares y las huellas almacenadas en la base de datos del terminal. Cuanto mayor sea el nivel, mayor es la seguridad, pero la posibilidad de fallo de autentificación es mayor.

El nivel de autentificación 1:1 se utiliza cuando la autentificación se lleva a cabo junto con un ID. Si el ID introducido es '1234 ', la huella digital registrada con el ID '1234' se recupera de la base de datos para comparar las dos huellas dactilares.

However, in the case of 1:1 authentication, if a user's 1:1 level is not set to [0] (1:1 level of the terminal is used), the user's 1:1 level is used.

Pulse [ENTER] para pasar al siguiente ajuste.

3.8.3.2. Verificación 1:N

◆[ENTER] → [6] → '084265' [ENTER] → [3] → [ENTER] ◆

Nivel 1:N (3-9):5

Valor por defecto: '5'

Ajusta el nivel de identificación cuando la autentificación se lleva a cabo sin entrada de ID.
Una huella digital introducida se compara con todas las huellas digitales en la base de datos para permitir la autentificación 1:N.

Para la autentificación 1:N, el nivel de identificación no se ha establecido para cada usuario, por lo que se utiliza un nivel de autentificación básico.

Pulse [ENTER] para pasar al siguiente ajuste.

3.8.3.3. Captura inteligente

<I-Capture> (N=0/Y=1):1

Valor predeterminado: '1'

Ajusta la configuración del sensor de forma automática para mejorar la capacidad de detección, independientemente de la suciedad que puedan

presentar las huellas dactilares (sudor, humedad residuos en el dedo).

- Si se pone a '0 ', el tiempo de autentificación de huellas digitales es más corto, pero la tasa de éxito es menor para las huellas digitales secas o húmedas.
- Si se establece a '1 ', tarda alrededor de 0,5 ~ 1 seg. Sin embargo, la tasa de éxito es mayor, por lo que se recomienda '1'.

Una vez que haya completado el ajuste, pulse [ENTER] para ir al menú superior.

3.8.4. Wiegand output settings

◆[ENTER] → [6] → '084265' [ENTER] → [4] ◆

Wiegand Out:0 0=None 1=26bit 2=34bit

Default setting: '0'

Cuando esto se pone a '1 ', "Código del Sitio + ID de usuario" se envía al puerto Wiegand del terminal cuando se realiza la autenticación. Se puede utilizar sólo para sistemas donde existe un controlador de bloqueo y el controlador está operado por una entrada de Wiegand. Valor por defecto a '0 '.

- Si se pone a '1 ', ID de usuario deberá ser inferior a 4 cifras porque "Código del lugar [1 byte] + ID de usuario [2 bytes]" se transfiere.
- Si se ajusta a '2 ', ID de usuario deberá ser inferior a 7 dígitos, porque "el código del sitio [1 byte] + ID de usuario [3 bytes]" se transfiere.

※Esto no es eficaz cuando se utiliza un lector de tarjetas de tipo Wiegand, y establece el siguiente código de sitio cuando el ajuste es mayor que '1'.

<Site Code> (0-255):000

Default setting: '000'

This is only available when Wiegand Out is set to '1' or '2'. Enter the site code (0-255) to be sent to the Wiegand Port together with the user ID.

<Bypass> (0=Off/1=On):1

Valor por defecto: '1'

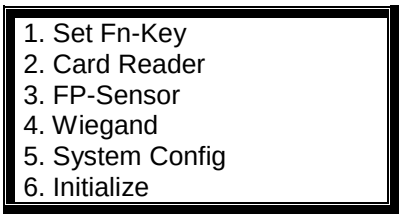
wiegand 카드 입력시 wiegand 카드값을 출력으로 하려면 '1' 로 설정하며, 위에 설정한 형태로 출력하려면 '0' 으로 설정한다.

* Bypass 를 '1'로 설정한 경우에도 지문사용자의 경우 설정한 형태로 출력한

다.

Una vez que haya completado el ajuste, pulse [ENTER] para ir al menú superior.

3.8.5. Configuración del sistema



Pulse [5] para configurar el sistema.

3.8.5.1. ID de usuario

◆[ENTER] → [6] → '084265' [ENTER] → [5] ◆

Valor por defecto: '4'

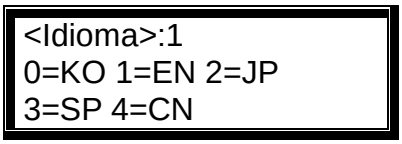
Se compone de un número de 2 ~ 8 dígitos y será el mismo que el ID registrado en servidor. Si el ID registrado en servidor es '000075 ', introduzca 6.

Se requiere especial cuidado cuando se reduce el número de dígitos durante una operación normal, ya que el administrador puede no ser autentificado cuando quiere entrar en los menús, debido al reducido número de dígitos.

Pulse [ENTER] para pasar al siguiente ajuste.

3.8.1.2. Idioma

◆[ENTER] → [6] → '084265' [ENTER] → [5] → [ENTER] ◆



Valor por defecto: '1' (Inglés)

La información de voz sigue estos valores: '0 ': coreano, '1': Inglés, '2 ': japonés, '3': español, '4 ': Chino.
'0 '~ 2 ": caracteres LCD también corresponden al idioma.
'~ '4' '3: caracteres LCD en Inglés.

Una vez que haya completado el ajuste, pulse [ENTER] para ir al menú superior.

3.8.6. Inicialización del terminal

En el menu principal, pulse [6] y seleccione “6. Dispositivo”. Aparecerá la siguiente pantalla:

1. Init Config 2. Delete Log 3. Init Terminal

Para inicializar los ajustes, pulse [1].
Para inicializar el registro, pulse [2].
Para los ajustes predeterminados de fabrica, pulse [3].

3.8.6.1. Inicialización de los ajustes

◆[ENTER] → [6] → ‘084265’ [ENTER] → [6] → [1] ◆

<Init Config> [Y=1 / N=2] :

Para inicializar los ajustes, pulse [1]. Si no, pulse [2].

Todos los ajustes se inicializan, excepto la dirección (física) Mac, pero no se eliminan los registros de usuarios u autentificación.

※ Si se inicializan los ajustes, el idioma de la voz y los menús se convierten en Inglés. Si necesita configurar otro idioma:
(". 6 Configuración del dispositivo" ◊ "1 Sistema Config." ◊ <Idioma>: establecer 0 ~ 4)

Una vez que la inicialización se realiza correctamente, se desplaza al menú superior junto con un sonido "ppiririck".

3.8.6.2. Inicialización del registro de autentificación

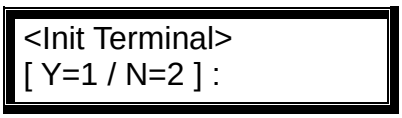
◆[ENTER] → [6] → ‘084265’ [ENTER] → [6] → [2] ◆

<Delete All Log> [Y=1 / N=2] :

Para inicializar el registro, pulse [1].
Si no, pulse [2].

Elimina todos los registros relacionados con la autentificación, pero no elimina los ajustes ni los usuarios.
Una vez que la inicialización se realiza correctamente, se desplaza al menú superior junto con un sonido "ppiririck".

3.8.6.3. Inicializacion de fabrica



Para los ajustes predeterminados de fábrica, pulse [1]. Si no, presione [2].

A excepción de la dirección Mac (física) almacenado en el terminal, todas las configuraciones, usuarios e información de registro se eliminan para el valor predeterminado de fábrica.

Si se inicializan los ajustes, el idioma y los menus cambian a Ingles. Si necesita configurar otro idioma:

(". 6 Configuración del dispositivo" ◊ "5 Sistema Config." ◊ <Idioma>: establecer 0 ~ 4)

Una vez que la inicialización se realiza con éxito, el terminal se reinicia y se escuchará un sonido "ppiririck".

4. Usos del terminal

4.1. Control de acceso

- Menu “3.Opciones” → “1.Aplicaciones” → [0] Configuración control de acceso

4.1.1. Modo de autentificación

- Visualización del modo de autentificación

Modo normal; autentificación con [ENTER]

Modo F1 ; autentificación con [F1]

Modo F2; autentificación con [F2]

Modo F3 ; autentificación [F3]

Modo F4 ; autentificación con [F4]

- Autentificación con huella dactilar
  Pulse la tecla de función para la autentificación con el modo correspondiente. Si la tecla de función no se utiliza y la autentificación se realiza con detección automática, se utiliza el modo de autenticación actual de la pantalla.
- Autentificación con contraseña
  Después de introducir el ID de usuario y cambiar el modo de autenticación pulsando la tecla de función correspondiente, introduzca una contraseña para

la autentificación.

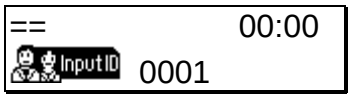
-When a card is used together (ej., menu → “6.Dispositivo” → “3.Lector de tarjeta” → cuando el lector de tarjetas está ajustado en más de 1.

Al ajustar la tecla de función, sólo cambia el modo de autenticación en lugar de entrar en la autenticación de huellas digitales, por lo que cambie el modo de autenticación pulsando la tecla de función correspondiente para introducir la tarjeta.

4.1.2. [1:1] Autentificación con huella dactilar

-Durante la detección automática, si el ID de usuario es '0001 ', introduzca '0001', y luego coloque el dedo cerca del sensor de huellas dactilares. La luz en la ventana de entrada de huellas dactilares se encenderá para detectar la huella y el resultado de la autentificación se mostrará en la ventana LCD.

▸ Si el ID de usuario es '0001 ', introduzca '0001' y pulse la tecla de función. La luz en la ventana de entrada de huellas digitales se enciende y se escuchará la información de voz. Cuando se introduce una huella digital, el resultado de la autenticación se mostrará en la ventana LCD.



Si el ID de usuario es '0001 ', introduzca '1' o '0001 'y pulse la tecla de función.

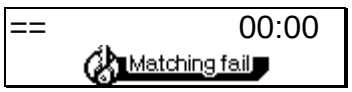
▼

Coloque el dedo sobre la ventana de entrada cuando la luz se encienda junto con el mensaje de voz "Introduzca su huella digital". No retire el dedo hasta que escuche un sonido "ppig".

▼

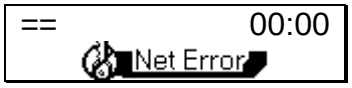
Si la autenticación se realiza correctamente, un mensaje de éxito se mostrará en la pantalla LCD junto con un mensaje de voz “Está autorizado". El relé de la puerta y la luz LED se encenderán.
Aparecerá la pantalla predeterminada después de 1 ~ 2 seg., Y el relé de la puerta y el LED se apagarán cuando haya transcurrido el tiempo configurado de puerta abierta.

※ Mensaje de error: Aparecerá junto con el mensaje “Por favor, vuelva a intentarlo”.



Error de autentificación.

ID de usuario no registrado.



Problemas de red durante la autentificación.

4.1.3. [1:N] Autentificación con huellas dactilares

Esta autenticación sólo se permite para un usuario que está registrado con la autentificación 1:N.

▸ Si un usuario coloca su dedo en el sensor de huellas digitales, la luz de la ventana se encenderá para detectar la huella y el resultado de la autenticación se mostrará en la ventana LCD.

▸ En la pantalla predeterminada, pulse la tecla de función y la luz de la ventana de entrada de huella digital se encenderá junto con un mensaje de voz "Introduzca su huella digital". Cuando coloque la huella sobre el sensor, el resultado de la autenticación se mostrará en la ventana LCD.

En la pantalla predeterminada, pulse la tecla de función.

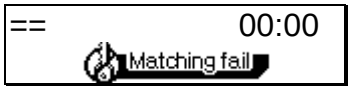
▼

Cuando se enciende la luz de la ventana de entrada de huellas digitales escuchará el mensaje de voz "Introduzca su huella digital". Coloque el dedo y manténgalo en esa posición hasta que escuche un sonido "ppig".

▼

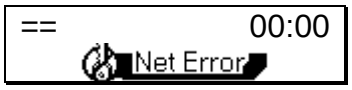
Si la autentificación se realiza correctamente, aparecerá un mensaje de confirmación en la pantalla junto con el mensaje de voz “Está autorizado". El relé de la puerta y el LED se encienderán.
Aparecerá la pantalla predeterminada después de 1 ~ 2 seg y el relé de la puerta y el LED se apagarán cuando haya transcurrido el tiempo configurado de puerta abierta.

※ Mensaje de error: Aparecerá junto con el mensaje “Por favor, vuelva a intentarlo”.



Error de autentificación.

Si el método de conexión es SN y no hay ningún usuario con autentificación 1:N.

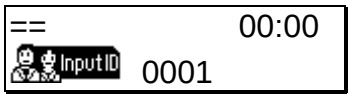


Problemas de red durante la autentificación.

▸ En el caso de un usuario registrado con huella digital y contraseña, se requiere una entrada de contraseña para una autentificación exitosa después de la autenticación de huella digital.

4.1.4. Autentificación con contraseña

Si el ID de usuario es "0001", introduzca "0001" y pulse la tecla de función. Oirá un sonido "ppiriririck" y deberá introducir una contraseña. Escribala y pulse [ENTER]. El resultado de la autenticación aparecerá en la pantalla LCD.



Si el ID de usuario es '0001 ', introduzca '0001' y pulse la tecla de función.

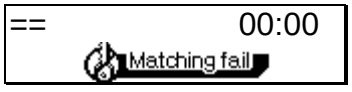
▼

Oirá un sonido "ppiriririck" y el terminal esperará la entrada de una contraseña de usuario. Introduzca la contraseña y pulse [ENTER].
(la contraseña se mostrará como "*" en la pantalla LCD, en lugar de los números reales.)

▼

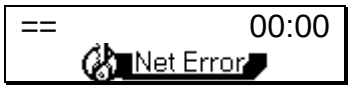
Si la autentificación se realiza correctamente, aparecerá un mensaje de confirmación en la pantalla junto con el mensaje de voz "Está autorizado". El relé de la puerta y el LED se encenderán.
Aparecerá la pantalla predeterminada después de 1 ~ 2 seg., y el relé de la puerta y el LED se apagarán cuando haya transcurrido el tiempo de configuración de puerta abierta.

※ Mensaje de error: Aparecerá junto con el mensaje “Por favor, vuelva a intentarlo”.



Error de autentificación.

ID de usuario no registrado.



Problemas de red durante la autentificación.

4.1.5. Autentificación con tarjeta

▸ Para un usuario registrado con [RF], [RF | FP], o [RF | PW], cuando coloque la tarjeta cerca de la pantalla, escuchará un sonido "ppig". El resultado de la autentificación aparecerá en la pantalla LCD.

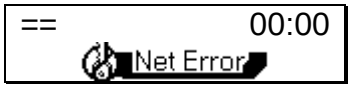
Si coloca su tarjeta cerca de la unidad, escuchará un sonido zumbador "ppig"

▼

Si la autentificación se realiza correctamente, aparecerá un mensaje de confirmación en la pantalla junto con el mensaje de voz "Está autorizado". El relé de la puerta y el LED se encenderán.
Aparecerá la pantalla predeterminada después de 1 ~ 2 seg., y el relé de la puerta y el LED se apagarán cuando haya transcurrido el tiempo de configuración de puerta abierta.

※ Mensaje de error: Aparecerá junto con el mensaje “Por favor, vuelva a intentarlo”.

Tarjeta de usuario no registrado.



Problemas de red durante la autentificación

▶ Para usuarios registrados con [RF&FP] o [ID&FP | RF&FP], al colocar la tarjeta cerca de la pantalla, se escuchará un sonido "ppig" y aparecerá la siguiente pantalla de autenticación de huellas digitales:

Cuando la luz de la ventana de entrada de huellas digitales se encienda, escuchará un mensaje de voz "Introduzca su huella digital". Coloque el dedo y manténgalo en esa posición hasta que escuche un sonido "ppig".

▶ Para usuarios registrados con [RF y contraseña] o [ID y contraseña | RF y contraseña], al colocar la tarjeta cerca de la pantalla, escuchará un sonido "ppig" y aparecerá la siguiente pantalla de autenticación de huellas digitales:

Escuchará un sonido "ppiriririck" y la unidad esperará la entrada de una contraseña de usuario. Introduzca la contraseña y pulse [ENTER].

4.1.6. Autentificación de ID de grupo

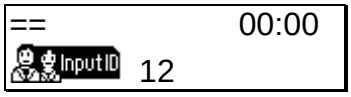
La autentificación se realiza con las primeras cifras (al menos un dígito) del ID de un usuario.

Es más conveniente que la autentificación 1:1. Se usa cuando la autentificación 1:N no se puede utilizar porque hay demasiados usuarios o cuando es demasiado lenta. Se ajusta de la siguiente forma:

3. Ajustes → 2. Métodos de autentificación → <Autentificación 1:N >=1 → <Autentificación ID de grupo >=1

Por ejemplo, para un usuario cuyo ID es 1234 ", durante la autentificación introduzca solamente '12. Aparecerán solamente las huellas digitales de los usuarios registrados entre el intervalo (1200 ~ 1299).

Si el ID es 0012 ', introduzca 0012' o '00 '.



Si el ID de usuario es ‘1234’, introduzca ‘1’, ‘12’, o ‘123’,y pulse la tecla de función.

▼

Cuando la luz de la ventana de entrada de huellas digitales se encienda, escuchará un mensaje "Introduzca su huella digital". Coloque su dedo y manténgalo en esa posición hasta que escuche un sonido "ppig".

▼

Si la autentificación se realiza correctamente, aparecerá un mensaje de confirmación en la pantalla junto con un mensaje de voz "Está autorizado". El relé de la puerta y el LED se encenderán.

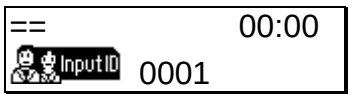
Aparecerá la pantalla predeterminada después de 1 ~ 2 seg., y el relé de la puerta y el LED se apagarán cuando haya transcurrido el tiempo configurado de puerta abierta.

4.1.7. Autentificación de huellas digitales múltiple

Para una puerta que requiera un mayor nivel de seguridad, se asigna más de múltiples huellas dactilares procedentes de más de 2 personas a un único ID. La puerta se abre sólo cuando todas las huellas dactilares registradas son autentificadas.
Se ajusta de la siguiente manera:
3. Opciones ◊ 2. Configuración del método de autentificación ◊ <Autentificación 1: N > = 0 ◊ <autenticación de huellas digitales múltiples> = 1

Por ejemplo, si el ID '0001 'se ha registrado con 3 huellas dactilares, todas deben ser autentificados después de la entrada del ID. Un solo fallo en el medio renueva el proceso de autenticación. Este proceso iterativo continúa hasta que las 3 huellas dactilares esten autenticadas.

Si el ID de usuario es '0001 ', introduzca '1' o '0001 'y pulse la tecla de función. La luz de la ventana de entrada de huellas digitales se encenderá y escuchará un mensaje de voz "Introduzca su huella digital." (Durante la detección automática, la entrada de la huella digital por sí sola es suficiente). El resultado de la autenticación se mostrará en la ventana LCD.



Si el ID del usuario es ‘0001’, introduzca ‘0001’ y pulse la tecla de función.

Cuando la luz de la ventana de entrada de huellas digitales se encienda, escuchará un mensaje de voz "Introduzca su huella digital". Coloque el dedo y manténgalo en esa posición hasta que escuche un sonido "ppig".

Si la autenticación se realiza correctamente, se escuchará un sonido "ppiririck". Se encenderá la luz de la ventana de entrada de huellas digitales y escuchará un mensaje de voz "Introduzca su huella digital". Este proceso iterativo continúa hasta que todas las huellas digitales introducidas hayan sido autentificadas.

Si la autenticación se realiza correctamente, aparecerá un mensaje de confirmación en la pantalla junto con el mensaje de voz "Está autorizado". El relé de la puerta y la luz LED se encendrán.

Aparecerá la pantalla predeterminada después de 1 ~ 2 seg., y el relé de la puerta y la luz LED se apagará cuando haya transcurrido el tiempo configurado de puerta abierta.

※Mensaje de error: mismo error que la autentificación [01:01].

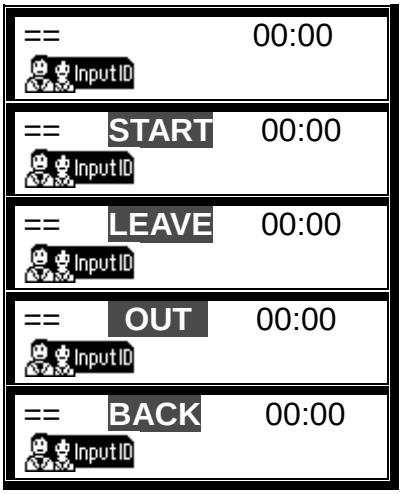
4.2. Control horario

- Menu “3.Opciones” → “1.Aplicaciones” → [1] T&A (Ajustes de control horario) settings

- Si la el tiempo de entrada / salida es fijo, ajuste<Entrada>, <Salida>, y <Tiempo Normal> para reducir los errores de entrada de usuarios.

4.2.1. Modo de autentificación

- Visualización del modo de autentificación



Modo normal; autentificación con [ENTER]

Modo entrada; autentificación con [F1]

Modo salida; autentificación con [F2]

Modo trabajo exterior, autentificación con [F3]

Modo regreso; autentificación con [F4]

- Autenticación de huellas dactilares

Pulse la tecla de función para la autenticación en modo de trabajo.
Si la tecla de función no se utiliza y la autenticación se realiza con detección automática, se utilizará el modo de autenticación actual de la pantalla.

- Autentificación con contraseña

Después de introducir el ID de usuario y cambiar el modo de autenticación pulsando la tecla de función correspondiente, escriba la contraseña para la autenticación.

-When a card is used together (i.e., Menu → 6.Device settings → 3. Card reader → when <Card Reader> is set to over 1)

When entering the function key, only the working mode is changed instead of

entering into fingerprint authentication, so change the working mode by pressing the corresponding function key to enter the card.

- El modo de trabajo después de la autentificación depende del tiempo que se haya ajustado para <Entrada> <salida>, y <tiempo normal>. El modo de autentificación anterior se mantiene si no hay modo ajustado para un período de tiempo específico.

4.2.2. Autentificación de huellas dactilares [1:1]
- el mismo que 4.1.2.

4.2.3. Autentificacion de huellas dactilares [1:N]
- el mismo que 4.1.3.

4.2.4. Autentificación con contraseña
- el mismo que 4.1.4.

4.2.5. Autentificación con tarjeta
- el mismo que 4.1.5.

4.2.6. Autentificación de ID de
- el mismo que 4.1.6.

4.2.7. Working mode expansion using multi-key authentication

- Si hay más de 5 modos de trabajo, tales como Entrada, Salida, Fuera trabajo o retorno, se puede ampliar hasta 41 modos.

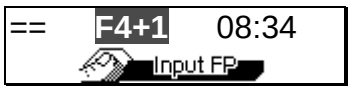
- Para configurar el Menú ◊ ◊ 3.Opciones- 1.Aplicaciones ◊ [1] T & A, en <Tecla multi-funcion>, se recomienda establecer más de una tecla a 'O'. However, the keys set to ‘X’ are not the case.

- Debido a que un modo se define con una tecla numérica, introduzca una tecla numérica después de entrar en la tecla de función para la autentificación. En el servidor, el modo de autentificación es "F3+1".

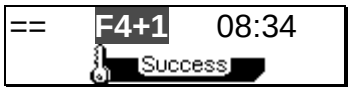
- Por ejemplo, cuando [F4] se ajusta a [O] y la <Entrada > se establece entre '07: 00 ~ 09:30 ', si un usuario intenta una autentificación de huellas digitales "F4 1",

En la pantalla predeterminada, pulse [F4].

Cuando el modo se cambia a “F4+0”.
Pulse [1].



Cuando el modo se cambia a “F4+1”, introduzca la huella dactilar.



Cuando la autentificación se complete exitosamente, aparecerá un mensaje de verificación.

La hora actual es 08:34, por lo que vuelve a la modalidad de arranque.